

## DOD PRIVACY IMPACT ASSESSMENT (PIA)

### **1. Department of the Army organizational name (APMS Sub Organization name)**

Army National Guard (National Guard Bureau)

### **2. Name of Information Technology (IT) System (APMS System name)**

Guard Electronic Medical Record (GEMR)

### **3. Budget System Identification Number (SNAP-IT Initiative Number)**

NA

### **4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR))**

7406

### **5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable)**

NA

### **6. Privacy Act System of Records Notice Identifier (if applicable).**

A0040-3a DASG, Medical Review Files (March 27, 2003, 68 FR 14959)  
A0040-400 DASG, Entrance Medical Examination Files (March 27, 2003, 68 FR 14954).  
A0601-210a USAREC, Enlisted Eligibility Files (December 8, 2005, 70 FR 72998).  
A0601-210 AHRC, Eligibility Determination Files (February 23, 2004, 69 FR 8183).  
A0601-270 USMEPCOM DoD, U.S. Military Processing Command Integrated Resources System (USMIRS) (February 25, 2005, 70 FR 9284).

### **7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.**

NA

### **8. Type of authority to collect information (statutory or otherwise).**

10 U.S.C. 504, Persons not qualified;  
10 U.S.C. 3013, Secretary of the Army;  
10 U.S.C. 5013, Secretary of the Navy;  
10 U.S.C. 8013, Secretary of the Air Force;  
10 U.S.C. Chapter 55, Medical and Dental Care;  
E.O. 9397 (SSN)

DoD Directive 1145.2, United States Military Entrance Processing Command;  
Army Regulation 40-3, Medical, Dental, and Veterinary Care;  
Army Regulation 40-501, Standards of Medical Fitness;  
Army Regulation 601-210, Regular Army and Army Reserve Enlisted Program;  
Army Regulation 601-270/Air Force Regulation 33-7/Marine Corps Order P1100.75A,  
Military Entrance Processing Station (MEPS);  
Army Regulation 601-280, Army Retention Program;  
Army Regulation 635-200, Enlisted Personnel;  
MEPCOM Regulation 680-3, U.S. Military Processing Command Integrated Resources  
System (USMIRS)

**9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).**

The system provides a web-based solution for the National Guard Bureau, Office of the Chief Surgeon, to receive and process requests for medical waivers from potential recruits. The automated system allows electronic receipt, storage, processing, retrieval and archive of all data and documents relevant to medical waiver requests. It eliminates repeated handling of paper documents.

GEMR is connected through the Internet to users in 54 states and territories using unclassified servers.

Backup images are stored in the data center; weekly and monthly data is backed up to tape.

**10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other Army IT systems, other component IT systems, IT systems from agencies outside DoD, etc.).**

Demographic information and protected health information. The system may accept data from more than one source

**11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).**

Information is collected through keyboard entry and by scanning paper documents.

**12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a DA program, etc.)**

The data is collected in order to document a potential recruit's condition of health and

fitness for serving in the National Guard. Variances from health and fitness standards become the prompt for requesting a waiver.

**13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).**

Information is used to identify the recruit to the Office of the Chief Surgeon and to assist that office in determining whether or not to grant a waiver for a physical condition.

**14. Describe whether the system derives or creates new data about individuals through aggregation.**

This system does not create new data about individuals through aggregation

**15. Describe with whom the information in identifiable form will be shared, both within DA and outside the DA (e.g., other Army organizations, other DoD Components, Federal agencies, etc.).**

Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

**16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.**

Potential recruits who do not wish to request a waiver are not required to do so and may decline to submit data required for a waiver. Consent to provide information entered into the system is obtained through a release memo signed by the potential recruit. No further release is required to send the waiver action to the requesting authority.

**17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory), as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.**

Waiver action is sent to the requesting authority via e-mail through the GEMR program.

**18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.**

The system is password protected based on user roles and access in accordance with Army Regulation 25-2, Information Assurance.

**19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004 and AR 340-21, Army Privacy Program, July 8, 1985. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.**

System of Record Notices are identified in Para 6 above.

**20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals.**

Sensitive information contained in the system is safeguarded in accordance with Army regulations and National Guard Bureau policies.

There is no risk in allowing individuals the opportunity to object or consent, or in notifying individuals.

**21. Describe/evaluate further any risks posed by the adopted security measures. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.**

Data in the system is sensitive and FOUO. The PIA may be published.